Overview of the ASDI Audit Process
Federal Aviation Administration
Traffic Flow Management Program Office
Version 1.2, March 13, 2008

Background

The Aircraft Situation Display to Industry (ASDI) Program has since 1992 been providing flight data to the private sector. This flight data includes flight plans, departure messages, airborne position reports updated once a minute, arrival messages, and other messages; see reference 1 for a description of this data. Over the years several dozen ASDI vendors have found many markets for this data and have created a rich set of applications that are sold to a wide variety of customers.

The Security Problem

The ASDI feed for the first ten years of its existence provided this data in what is called near real-time. That is, the data was typically received by the ASDI vendors a few seconds after it was generated by the Host computers at the en route centers. Because the delay in receiving this data is so short, it is called the undelayed feed.

After September 11, 2001, there were some in the security community who advocated that the ASDI feed be shut down since the near real-time data, if it fell into the wrong hands, could be used to attack aircraft. This left the FAA with a dilemma. On the one hand, the FAA needed to deal with the security problem that could result if ASDI data fell into the wrong hands. On the other hand, the ASDI data had enabled a large and thriving industry to spring up that met a real need, and the FAA needed to make sure that this industry and the benefits that it provided to the public were not needlessly harmed.

The Solution to the Security Problem

After much discussion and debate, the FAA decided that the solution to this security problem lay in distinguishing between two classes of users of the data. *Class One users* consist of the relatively narrow segment of users that need the data for their aviation operations. Roughly speaking, Class One users include airlines and any other organizations that dispatch flights. *Class Two users* consist of all users who are not Class One users. Class Two users include a vast array of users of the aviation data such as travel agents, limousine companies, financial analysis companies, and many others. Also, the term *direct subscriber* refers to any organization that gets the data directly from the FAA; an *indirect subscriber* is anyone who gets the data from a direct subscriber or another indirect subscriber rather than directly from the FAA. A *Class One direct subscriber* is a direct subscriber who passes the data to at least one Class One user. A *Class Two direct subscriber* is a direct subscriber who passes the data only to Class Two users. (For a more precise definition of the italicized terms in this paragraph, see section 5 of reference 2.)

This method that the FAA has used for the last few years to handle the ASDI feed's security problem can be summarized in the following way.

- Class One users are allowed to receive the near real-time feed. The thinking is that these users need the undelayed feed in order to operate efficiently.

- Class Two users are only allowed to receive a delayed version of the feed. The thinking is that these organizations can operate satisfactorily if they receive the feed with a delay.
- All direct subscribers must sign a memorandum of agreement (MOA, see reference 2). This MOA spells out in detail the special steps that the Class One direct subscribers must take to protect the sensitive, undelayed data. Since the Class Two direct subscribers receive only the delayed data, which is not seen as sensitive, the conditions imposed on the Class Two direct subscribers are much less restrictive.
- A successful audit must be on file with the FAA before a direct or indirect Class I subscriber is eligible to receive undelayed data.
- To ensure that the Class One direct subscribers treat the undelayed data in a way that protects it, the FAA requires that they undergo an annual audit that verifies that they are adhering to the required restrictions.

Adjustments to the Way the Security of the ASDI Feed is Safeguarded

The FAA now has several years of experience with the solution of the security problem sketched above. For the most part, this solution has been found to be satisfactory, and it does not need a complete reworking; experience, however, shows that some adjustments are needed.

In the original plan, only the ASDI direct subscribers were required to sign the MOA (Class One and Two) and undergo the annual audit (Class One). While this plan is good as far as it goes, some of the vendors distribute the undelayed feed to indirect subscribers, and the FAA recognized that assurance was needed that these indirect subscribers were treating the data with proper care.

Therefore, the FAA is making the following adjustments to its security plan.

- Any organization that receives Class One undelayed data must sign a MOA. Direct subscribers must sign a MOA with the FAA. It is the responsibility of the Direct Subscriber of Class One data to ensure that they have an executed MOA on file with their Indirect Subscribers of Class One data at all levels. The FAA may, at its discretion, request copies of executed Indirect Subscriber MOAs. See attachment 1 for an example of a MOA for an Indirect Subscriber. Previously, only direct subscribers had been required to sign the MOA. This change, for example, implies that if an airline gets the undelayed feed, then the airline would need to sign the MOA; previously, this airline was not required to sign the MOA.
- Any organization, whether a direct or indirect subscriber, that receives the undelayed data must undergo an annual audit. It is the responsibility of the Direct Subscriber of Class One data to ensure that their indirect subscribers have undergone the required audit. The FAA may, at its discretion, request copies of Indirect Subscriber audits. Previously, only direct subscribers had been required to undergo the audit. This change, for example, implies that if an airline gets the undelayed feed, then the airline would need to undergo an audit; previously, this airline was not required to undergo an audit.
- The audit guidelines have been revised. One reason for this revision is increased clarity. That is, these guidelines should both specify to the auditors what they must audit and also inform the audited party what it must do to protect the data and pass the audit; there should not be doubt in anyone's mind about what the audit will cover. Another reason for the revision of the audit guidelines is to allow different levels of audit. Rather than having one audit apply to all recipients of the undelayed feed, the level of audit is tailored to each user's amount of risk; this is discussed further below.

Two aspects of the original plan remain unchanged.

- A direct subscriber that only receives the delayed feed must sign the MOA but it does not need to undergo the annual audit. This means that if a direct subscriber finds the audit too expensive or burdensome, it can avoid it by foregoing the undelayed feed and instead getting the delayed feed.
- An indirect subscriber who only receives the delayed feed does not need to sign a MOA with their direct subscriber and does not need to undergo an audit. This means that if an indirect subscriber finds the audit too expensive or burdensome, it can avoid it by foregoing the undelayed feed and instead getting the delayed feed.

In short, the philosophy behind these adjustments to the audit process is: Because the undelayed data is high-profile and sensitive, all organizations that receive it must demonstrate that they are treating it with sufficient care; they do this by signing the MOA and by undergoing the annual audit to demonstrate that they are in compliance with the MOA.

Who Needs What Kind of Audit?

The FAA realizes that the requirement of the annual audit will impose a cost, and the FAA is eager to keep the cost as low as possible, consistent with the need to maintain security. To minimize this cost, the FAA is taking the approach of having three levels of audit (full, reduced, and minimal) and of only requiring each recipient of the undelayed data to undergo the least expensive audit that is consistent with its use of the data. The five rules for determining what kind of an audit a subscriber is required to undergo are as follows.

1. *RULE #1: Any direct subscriber who receives the undelayed feed must undergo the **full audit**.* The thinking is that since this subscriber connects directly to the FAA and receives the sensitive, undelayed feed, the full audit is justified. This full audit is roughly equivalent to the audit that has been required for the last few years. See reference 3 for a description of the full audit.

2. *RULE #2: Any subscriber, even an indirect subscriber, who receives undelayed data and distributes ASDI data, whether undelayed or delayed, outside of its organization must undergo the **full audit**.* The thinking is that since this subscriber has undelayed data and since it is distributing data, it is at risk and the full audit is justified.

(If an indirect subscriber receives the data, a distinction is whether that data is in what is called *digital format* or *display-only format*. If the data is in digital format, then this means that the data can be processed, and it is more open to theft. If the data is in display-only format, this means that the subscriber can look at the data, e.g., in a web page, but does not have scope for processing it.)

3. *RULE #3: An indirect subscriber who receives undelayed data in digital format but does not distribute it is required to undergo the **reduced audit**.* The thinking is that the full audit is not needed since the data is not distributed and since an indirect subscriber does not connect directly to the FAA servers; nevertheless, a serious audit is still needed since this subscriber is handling the sensitive, undelayed data in digital form. See reference 4 for a description of the reduced audit.

4. *RULE #4: An indirect subscriber who receives undelayed data in display-only format but does not distribute it is required to undergo the **minimal audit**.* The minimal audit would be a self-audit in which the subscriber would go through a check-list and provide the results to the direct subscriber. See reference 5 for a description of the minimal audit.

5. *RULE #5: Any subscriber, whether direct or indirect, who receives delayed data is not required to undergo an audit.*

Table 1 summarizes the rules for determining the type of audit that is required for direct subscribers. Table 2 summarizes the rules for determining the type of audit that is required for indirect subscribers; each line in this table summarizes one of the above rules. The first four columns of this table show characteristics of the indirect subscriber, where a hyphen indicates that the characteristic does not matter. The last column shows the type of audit that is required for each set of characteristics.

Table 1: Summary of Audit Requirements for ASDI Direct Subscribers

Undelayed Data	**Required Audit**
Y	Full
N	None

Table 2: Summary of Audit Requirements for ASDI Indirect Subscribers

Undelayed Data	**Distributes Data**	**Receives Digital Data**	**Receives Display-only Data**	**Required Audit**
Y	Y	-	-	Full
Y	N	Y	-	Reduced
Y	N	N	Y	Minimal
N	-	-	-	None

The audit requirements are shown graphically in Figure 1.

Figure 1: Illustration of Different Subscribers and the Level of Audit Required

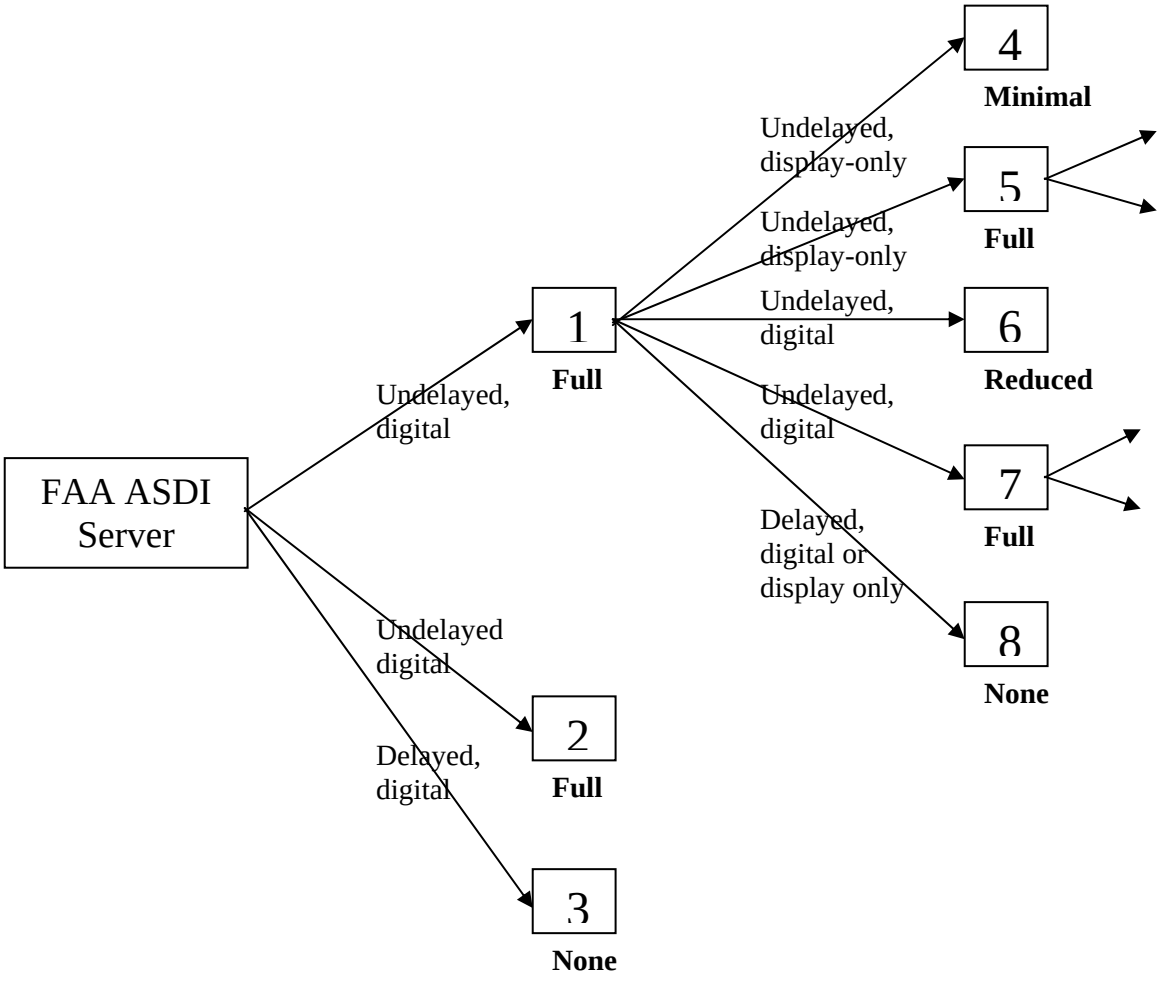

Figure 1 shows eight example ASDI subscribers and the following information about each.

- Whether the subscriber is directly connected to the FAA ASDI servers.
- Whether the subscriber receives a delayed or an undelayed feed.
- Whether the subscriber receives a digital or a display-only feed.
- Whether the subscriber distributes the data outside of its organization.
- The level of audit that is required.

The required audit of each of these eight subscribers is determined in the following way.

1. Since this subscriber receives the undelayed feed directly from the FAA, a full audit is required. See rule 1. (That this subscriber distributes the data is a second reason why a full audit is required. See rule 2.)
2. Since this subscriber receives the undelayed feed directly from the FAA, a full audit is required. See rule 1. That it does not distribute is irrelevant.
3. Since this subscriber receives the delayed feed, no audit is required. See rule 5.
4. Since this subscriber receives an undelayed, display-only feed and does not distribute, a minimal audit is required. See rule 4.
5. Though this subscriber receives an undelayed, display-only feed, a full audit is required since it distributes. See rule 2. (It might well be that there are no subscribers in this category, but it is included for completeness.)
6. Since this subscriber receives an undelayed, digital feed and does not distribute, a reduced audit is required. See rule 3.
7. Since this subscriber distributes, a full audit is required. See rule 2.
8. Since this subscriber receives the delayed feed, no audit is required. See rule 5.

References

1. "Aircraft Situation Display to Industry: Functional Description and Interface Control Document," Volpe Center, report no. ASDI-FD-001, version 5.4, 15 November 2005. This document describes the ASDI feed and the messages that are included in it.

2. "Memorandum of Agreement for Industry Access to the Aircraft Situation Display and National System Status Information Data," Federal Aviation Administration, June 1, 2006. This document, which must be signed by the ASDI direct subscriber, spells out the responsibilities of both the FAA and the direct subscriber. If the direct subscriber violates this MOA, then the direct subscriber is liable to lose access to the feed. Any indirect subscriber who receives the undelayed feed must sign an agreement with their direct subscriber.

3. "ASDI Full Audit Guidelines," Version 1.1, June 20, 2007. This document describes the full audit.

4. "ASDI Reduced Audit Guidelines," Version 1.1, June 20, 2007. This document describes the reduced audit.

5. "ASDI Minimal Audit," Version 1.1, June 20, 2007. This document describes the minimal audit.

For the latest versions of these and other ASDI documents, go to http://www.fly.faa.gov/ASDI/asdi.html.

Contacts

For more information about the ASDI Program, contact the ASDI Program Office at asdi-program-office@faa.gov.

Appendix 1. Example of MOA for Indirect Subscriber

Memorandum of Agreement

For Indirect Subscriber Access to Class One

Aircraft Situation Display and National Airspace System Status Information Data

[date]

1. Parties

This Memorandum of Agreement (MOA) is entered into by and between _____ Insert name of Direct Subscriber) and _____, hereafter referred to as an Indirect Subscriber (and a recipient of Class One data as defined in Section 4 below). The parties do hereby agree and obligate themselves to abide by the rights, responsibilities, and other conditions defined in this agreement.

2. Purpose

This MOA addresses the requirement that all recipients of Class One data sign a MOA. To better manage the program, this MOA will be used for those indirect subscribers who receive Class One data. The rights, responsibilities, and other conditions for the Federal Aviation Administration (FAA) and the Indirect Subscribers who receive Class One ASDI and NASSI data are defined in the Direct Subscriber's MOA executed with the FAA (ASDI MOA)..

3. Definitions

3.1 Class One User:

A Class One User is a professional aviation organization with an established flight dispatch or planning function that requires near real time positional flight-tracking capabilities. This organization must have direct responsibility for dispatching or tracking aircraft it owns or be contracted by the owner of the aircraft to do so. Examples are airlines, regional air carriers, air taxis, any organization providing dispatch or tracking functions for aircraft owners, flight operation centers, government users (as described in Section 5.5 of the ASDI MOA), and professional flight planning service providers.
Fixed Base Operators (FBOs), corporate flight departments, and part 135 operators must have direct responsibility for dispatching or tracking aircraft to qualify as a Class One User. The FAA shall be the final arbiter for any disputes regarding the interpretation of this Section.

3.2 Indirect Subscriber:

An Indirect Subscriber is an entity that receives the ASDI/NASSI data but not directly from the FAA. Indirect Subscribers that redistribute data received from Direct Subscribers (or from other Indirect Subscribers) are subject to the same requirements and restrictions as the Direct Subscriber, as detailed in ASDI MOA section 7.2 (dated 6/1/2006). If an Indirect Subscriber receives Class One data, that Indirect

Subscriber will be subject to the audit in accordance with ASDI MOA section 7.2.12. However, Indirect Subscribers that receive and redistribute only Class Two data are not subject to the audit requirement.

3.3 Data Access:

Class One Users are authorized to receive the full near real time ASDI and/or NASSI data feed (Class One data). Class Two Users are only authorized to receive the full ASDI and/or NASSI data feed that has been time-delayed at least 5 minutes (Class Two data). Government organizations and aviation system research and development industries will be categorized by the FAA on a case-by-case basis. Access and use restrictions for non-United States domestic ASDI/NASSI data are provided in section 10 of the ASDI MOA. Direct Subscribers may access ASDI data only (or a subset thereof), NASSI data only (or a subset thereof), or both ASDI and NASSI data (or subsets thereof).

4. Scope

This MOA addresses the requirement that all recipients of Class One data sign a MOA to insure compliance with restrictions on Class One data. The Indirect Subscriber who receives Class One data shall comply with the provisions identified in the ASDI MOA dated June 1, 2006, as they apply to indirect subscribers.

5. Signatures

Indirect Subscriber – Class One Data Recipient	**Direct/Indirect Subscriber**
Signature	Signature
Name (Printed)	Name (Printed)
Title	Title
Date	Date